UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/823,387	03/29/2001	Lebin Cheng	10010859-1	7378

7590   10/20/2004

HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER
SCHUBERT, KEVIN R

ART UNIT	PAPER NUMBER
2137	

DATE MAILED: 10/20/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)
Office Action Summary	09/823,387	CHENG, LEBIN
	Examiner	Art Unit
	Kevin Schubert	2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on _29 March 2001_.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) _1-20_ is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) _1-20_ is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on _29 March 2001_ is/are: a)☒ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _3/29/2001_.

4)☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

Claims 1-20 have been considered.

Specification

5   The disclosure is objected to because of the following informalities: The word "Standard"

in the third paragraph of the summary of the invention is erroneously capitalized. Appropriate

correction is required.

Claim Objections

10   Claim 8 is objected to because of the following informalities: a grammatical error exists.

The phrase "is conflict" should be replaced by "is in conflict". Appropriate correction is required.

Claim Rejections - 35 USC § 112

2nd Paragraph

15   The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and
> distinctly claiming the subject matter that the applicant regards as his invention.

Claim 10 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for

20   failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention. The applicant claims that one of the network types is an abstract type, but it is

unclear to the examiner whether the applicant wishes to claim that at least one network type is

abstract or exactly one network type is abstract. Appropriate correction is required. .

25   *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

5
(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-4,13,15,17,18, and 20 are rejected under 35 U.S.C. 102(b) as being

anticipated by Nessett, U.S. Patent No. 5,968,176.

10

As per claims 1 and 20, Nessett discloses a method of configuring a network security

system comprising:

a.   forming a registry data structure for defining roles within a network (Col 5, lines

27-37);

15
b.   mapping network security policies to the registry data structure, said network

security policies being contained in one or more policy documents stored in machine readable

form (Col 4, lines 10-14; Col 24, lines 38-40);

c.   using a document transformation algorithm to transform the policy documents

into one or more device-specific configuration documents stored in machine-readable form (Col

20   4, lines 14-20).

As per claim 2, Nessett discloses the method according to claim 1, further comprising

generating instances of the roles and associated security policies, each instance being mapped

to physical segments of the network (Col 5, lines 50-56).

25

As per claim 3, Nessett discloses the method according to claim 1, further comprising

distributing the device-specific configuration documents to network entities for implementing the

network security policies (Col 3, lines 22-32).

5   As per claim 4, Nessett discloses the method according to claim 1, wherein the registry

data structure comprises a collection of documents that include information regarding the

network roles and topology of the network (Col 5, lines 27-37; Col 7, lines 17-20).

As per claim 13, Nessett discloses the method according to claim 1, wherein the security

10   policies are representative of restrictions to be placed on one or more of the network roles in the

registry data structure (Col 3, lines 29-40).

The application should note that the management and enforcing of the security policies

necessitates that restrictions would have to be placed on one or more network roles.

15   As per claim 15, Nessett discloses the method according to claim 1, wherein the

document transformation algorithm is specific to a network entity utilized for implementing one

or more of the security policies contained in the policy documents (Col 9, lines 33-41).

As per claim 17, Nessett discloses the method according to claim 16, wherein the script

20   is specific to a network entity (Col 4, lines 47-55; Col 9, lines 33-38).

As per claim 18, Nessett discloses the method according to claim 16, further comprising

a step of selecting a script from among a plurality of scripts, each being specific to a different

network entity (Col 4, lines 47-55).

The applicant should note that Nessett discloses that depending on which script is selected, the topology data structure gives instruction as to which network entities can deal with the script. Thus, various scripts are specific to network entities.

5   *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject
10
> matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

15   Claims 5-9,11,12,14,16, and 19 are rejected under 35 U.S.C. 103(a).

Claims 5-9,11, and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in further view of The Open Group (The Open Group; "Authentication and Security Services- Introduction to Security Services"; 1997; Pages 44-56). Claims 14 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in further view of Cheung
20   (Cheung, Lee S., Lee T, Song, Tan; Distributed and Scalable XML Document Processing Architecture for E-Commerce Systems; 8-9 June 2000; Proceedings Second International Workshop on Advanced issues of E-Commerce and Web-Based Information Systems). Claim 19 is rejected under 35 U.S.C. 103(a) as being unpatentable over Nessett in further view of Cheung in further view of Kay (Kay, Michael H; XSLT Programmer's Reference, chapter "XSLT
25   Part 2- How Does XSLIT Transform XML?"; 20 February 2001. Wrox Books).

As per claim 5, the applicant discloses the claim limitation of claim 1, which is met by Nessett, with the following limitation which is met by The Open Group:

wherein the registry data structure comprises a hierarchy of network types, each type comprising a definition of a network role;

The Open Group illustrates how using a hierarchy to lay out a registry data structure is an effective way to store information (page 56). The hierarchy as described by The Open

5   Group is an effective way to store information because it allows for mapping of responsibilities between a parent and its children. In this manner it allows information to be managed effectively because the information is arranged structurally. It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with the ideas of Nessett and use a hierarchy of network types to effectively store

10   information.

As per claim 6, the applicant discloses the limitation of claim 5, which is met by Nessett in further view of The Open Group, with the following limitation which is met by Nessett:

wherein each network role is representative of a set of applications to be supported by

15   the network (Col 5, lines 27-37; Col 7, lines 17-20);

Nessett discloses the use of network roles or nodes which have identifying traits such as "the type of security policy that the node is able to enforce, the constructs used to enforce policy...and connection of the node to other nodes in the network" (Col 5, lines 35-38). Nessett shows that network roles or nodes are representative of a set of applications to be supported by

20   the network. Nessett, however, fails to specify the hierarchical framework that these roles or nodes could be placed in. The Open Group provides motivation to use a hierarchy because, as they claim, it is easy to manage data in this format. Thus, it would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of Nessett with

those of The Open Group to have network roles, which are in a hierarchical fashion,

representative of a set of applications to be supported by the network.

As per claim 7, the applicant discloses the claim limitation of claim 5, which is met by

5   Nessett in further view of The Open Group, with the following limitation which is met by The

Open Group:

wherein when a parent network type is mapped to a policy contained in one of the policy

documents, a child network type of the parent network type inherits the policy;

The Open Group describes a method whereby policies associated with a parent network

10   type are mapped to an inheriting child network type (pages 44-45) for security purposes. It

would have been obvious to one of ordinary skill in the art at the time the invention was filed to

combine the ideas of The Open Group with the ideas of Nessett and map the policies of the

parent network type to the child network type for security.

15   As per claim 8, the applicant discloses the limitation of claim 7, which is met by Nessett

in further view of The Open Group, with the following limitation which is met by The Open

Group:

wherein when the child network type is mapped to a policy contained in one of the policy

documents that is [in] conflict with the policy inherited from the parent, the policy mapped to the

20   child takes precedence over the policy inherited from the parent;

The Open Group discloses an inheritance system whereby the child type inherits its

data, such as its access control list (ACL), from the parent by default. The Open Group goes on

to claim that "if any of these ACLs are specified, they override the corresponding default [to the

parent]" (page 45). It would have been obvious to one of ordinary skill in the art at the time the

invention was filed to have combined the ideas of The Open Group with those of Nessett to

create a hierarchical system where policies mapped to a child take precedence over those

mapped to a parent if specified so that a user's mapping takes precedence over default

mapping.

5

As per claim 9, the applicant discloses the limitation of claim 5, which is met by Nessett

in further view of The Open Group, with the following limitation which is met by Nessett:

wherein an instance of one of the network types is mapped to one or more physical

network segments and wherein the network type includes a set of data fields for defining the

10   physical network segments;

Nessett discloses a system whereby security policies are mapped to network devices

which enforce the policies: "The multilayer firewall also includes a collection of network devices

that are used to enforce the defined policy. The security functions operating in this collection of

network devices across multiple protocol layers are coordinated by the policy definition

15   component so that particular devices enforce that part of the policy pertinent to their part of the

network" (column 3, lines 34-40). It would have been obvious to one of ordinary skill in the art at

the time the invention was filed to combine the ideas of Nessett with the ideas of The Open

Group because mapping security policies to network devices is an effective way to maintain

security in a system.

20

As per claim 11, the applicant discloses the limitation of claim 5, which is met by Nessett

in further view of The Open Group, with the following limitation which is met by The Open

Group:

wherein each network type further comprises a data field for identifying a human administrator;

The Open Group discloses a hierarchical model of nodes in a security system whereby a user, or client, can manipulate the nodes by entering certain data which is recognized by the

5   nodes (page 56). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to combine the ideas of The Open Group with those of Nessett so that one can add a data field for identifying a human administrator to the network nodes so that they can be manipulated by a user.

10   As per claim 12, the applicant discloses the limitation of claim 5, which is met by Nessett in further view of The Open Group, with the following limitation which is met by The Open Group:

wherein each network type further comprises a data field for providing a human readable description of the network type;

15   The Open Group discloses a hierarchical structure of nodes in a security system whereby a client can manipulate the system by referring to a node by name (page 56). It would have been obvious to one of ordinary skill in the art at the time the invention was filed to have combined the teachings of The Open Group with the teachings of Nessett to add human readable descriptions to network types.

20   As per claim 14, the applicant discloses the limitation of claim 1, which is met by Nessett, with the following limitation which is met by Cheung:

wherein the policy documents are in extensible markup language (XML);

Cheung discloses that XML is a good format to use because XML is an open and

scalable format for storing and exchanging data. Cheung also writes that XML is a good choice

for a distributed and scalable system (Cheung 1 Introduction, 1st paragraph). It would have

been obvious to one of ordinary skill in the art at the time the invention was filed to combine the

5   ideas of Cheung with the ideas of Nessett and use XML format for the policy documents.

As per claim 16, the applicant discloses the limitation of claim 15, which is met by

Nessett, with the following limitation which is met by Cheung:

wherein the document transformation algorithm includes style sheet language for

10   transformation (XSLT) controlled by a script;

Cheung discloses that XML is a good format to use because XML is an open and

scalable format for storing and exchanging data. Cheung also writes that XML is a good choice

for a distributed and scalable system (Cheung 1 Introduction, 1st paragraph). Furthermore,

Cheung illustrates that XSLT is an efficient way to convert one XML document to another

15   (Cheung 3.1.1 XML Transformation, 1st paragraph). It would have been obvious to one of

ordinary skill in the art at the time the invention was filed to combine the ideas of Cheung with

the ideas of Nessett and use XSLT to transform XML documents.

As per claim 19, the applicant discloses the limitation of claim 16, which is met by

20   Nessett in further view of Cheung, with the following limitation which is met by Kay:

wherein the device-specific configuration documents are in plain text format.

Kay writes in the first paragraph, "The data structure that results from the first stage can

be output as HTML, a text file or as XML...Plain text output allows data to be formatted in the

way an existing application can accept". It would have been obvious to one of ordinary skill in

the art at the time the invention was filed to have combined the teachings of Nessett and

Cheung with the teachings of Kay and make the output format for the device-specific

configurations to be plain text so that they are in an acceptable format for the applications.

5

Any inquiry concerning this communication or earlier communications from the examiner

should be directed to Kevin Schubert whose telephone number is (571) 272-4239. The

examiner can normally be reached on M-F 8:00-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

10   supervisor, Andrew Caldwell can be reached on (571) 272-3868.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system. Status information for published applications

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished

applications is available through Private PAIR only. For more information about the PAIR

15   system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private

PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

***

20

Andrew Caldwell

25